

Cited Reference

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-144059

(43) 公開日 平成11年(1999)5月28日

(51) Int.Cl.⁶
G 0 6 T 7/00
1/00

識別記号

F I
G 0 6 F 15/62
15/64

4 6 0
G

審査請求 未請求 請求項の数6 O.L (全9頁)

(21) 出願番号 特願平9-304518

(22) 出願日 平成9年(1997)11月6日

(71) 出願人 592044813

株式会社エニックス
東京都渋谷区代々木4丁目31番8号

(72) 発明者 福嶋 康博
東京都渋谷区代々木四丁目31番8号 株式
会社エニックス内

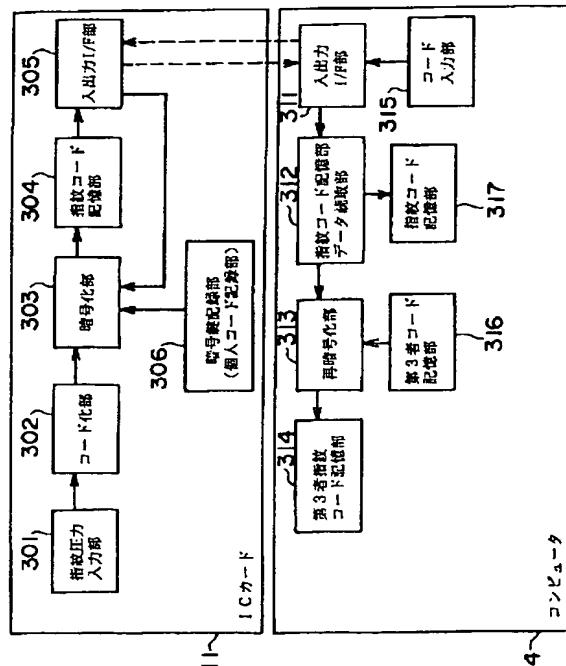
(74) 代理人 弁理士 小岩井 雅行 (外2名)

(54) 【発明の名称】 指紋登録システム

(57) 【要約】

【課題】指紋センサを組み込んだ指紋照合システムにおける指紋データの機密保持を図ることのできる指紋登録システムを提供すること。

【解決手段】指紋登録システムによると、指紋センサ12によって検出された指紋パターンは、コード化手段302によってコード化され、暗号化手段303によって暗号化され、記録手段304によって記録される。このように、指紋コードが暗号化されるので、個人の指紋コードを他人に知られることなく指紋照合システムを利用することができる。



【特許請求の範囲】

【請求項1】指紋パターンを検出する指紋センサと、前記指紋センサによって検出された指紋パターンをコード化するコード化手段と、前記コード化手段によってコード化された指紋コードを暗号化する暗号化手段と、前記暗号化手段によって暗号化された指紋コードを記録する記録手段とを備えたことを特徴とする指紋登録システム。

【請求項2】前記暗号化手段は、所定の個人コードを暗号鍵として前記指紋コードを暗号化することを特徴とする請求項1記載の指紋登録システム。

【請求項3】前記コード化手段によって指紋コードが生成される指と異なる同一人の他の指の指紋コードを記録した暗号鍵記録手段をさらに備え、前記暗号化手段は、前記コード化手段によって指紋コードが生成された際に、前記暗号鍵記録手段に記録された前記他の指の指紋コードを暗号鍵として生成された指紋コードを暗号化することを特徴とする請求項1記載の指紋登録システム。

【請求項4】前記暗号化手段によって暗号化された指紋コードである暗号化コードを再暗号化する再暗号化手段をさらに備えたことを特徴とする請求項2又は3記載の指紋登録システム。

【請求項5】前記再暗号化手段は、所定の第3者コードを暗号鍵として前記暗号化コードを再暗号化することを特徴とする請求項4記載の指紋登録システム。

【請求項6】前記第3者コードを記録した第3者コード記憶手段をさらに備えたことを特徴とする請求項5記載の指紋登録システム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、指紋センサを組み込んだ指紋照合システムを構成する指紋登録システムに関する、指紋コードの利用について有効な技術に関する。

【0002】

【従来の技術】従来、指紋データを検出し、その指紋データに基づいて本人照合を行う指紋照合システムが知られている。この種の指紋照合システムでは、指紋センサによって検出した個人の指紋パターンをコード化して指紋コードを取得し、この指紋コードと事前に登録された当該個人の指紋コードとを比較し、双方が合致すれば本人と判定する。

【0003】このような指紋照合システムが個人の範囲での利用、例えば個人の住宅の鍵や個人所有車のドアの開閉等に使用される場合には、個人の指紋データが他人へ漏れることは一般にはない。

【0004】

【発明が解決しようとする課題】しかしながら、指紋照合システムがクレジットカードや電子マネー等の本人照

合手段として用いられる場合には、個人の指紋データは、ICカード内部、或いは、クレジットカード会社や電子マネーの取引先等に設置されたコンピュータ内部に記録される。

【0005】このため、クレジットカード会社や電子マネーでの取引先等において、ICカードやコンピュータを介して重要なプライバシーである個人の指紋データが知られてしまうことが考えられる。このことは、指紋照合システムの普及に大きな障害となり得る。

【0006】また、上述したクレジットカード会社等は、本人照合のために多数の個人の指紋データをコンピュータを介して取り扱うことになるので、クレジットカード会社等から個人の指紋データが漏洩することも危惧される。

【0007】本発明はこのような点に鑑みてなされたものであり、指紋センサを組み込んだ指紋照合システムにおける指紋データの機密保持を図り、当該システムを広く普及させることができ可能な指紋登録システムを提供することを課題とする。

【0008】

【課題を解決するための手段】本発明は、上述した課題を解決するために以下の構成を採用する。すなわち、請求項1の発明は、指紋パターンを検出する指紋センサと、前記指紋センサによって検出された指紋パターンをコード化するコード化手段と、前記コード化手段によってコード化された指紋コードを暗号化する暗号化手段と、前記暗号化手段によって暗号化された指紋コードを記録する記録手段とを備えたことを特徴とする指紋登録システムである。

【0009】請求項1の発明によると、指紋センサによって検出された指紋パターンは、コード化手段によってコード化され、暗号化手段によって暗号化され、記録手段によって記録される。従って、個人の指紋コードを他人に知られることなく指紋照合システムを利用することが可能となる。

【0010】ここに、指紋センサは、指紋パターンを得ることができれば、どのような原理によるセンサでも良いが、特に、特開平6-28845(特許第2030279号)等に記載されている圧力式指紋センサを用いるのが好ましい。

【0011】また、指紋パターンをコード化するとは、例えば、指紋センサにより読み取った指紋パターンからマニューシャポイントと呼ばれる複数の特徴点を抽出し、各々の特徴点の相対位置等を数値化することを意味する。

【0012】また、指紋コードを暗号化するとは、例えば、指紋パターンをコード化したものに所定の行列式等を掛けることを意味する。このとき、暗号化した指紋コードから元の指紋コードを得るには、暗号化されたものに所定の逆行列式を掛ければ良い。

【0013】また、コード化手段や暗号化手段は、CPU(MPU)がプログラムを実行することによる機能として実現できる。また、記録手段は、例えば、RAM、フロッピーディスク、ハードディスク、光磁気ディスクなどで構成できる。

【0014】請求項2の発明は、請求項1記載の暗号化手段が、所定の個人コードを暗号鍵として前記指紋コードを暗号化することで特定したものである。請求項2の発明によれば、指紋コードに個人コードを暗号鍵として暗号化を図ることにより、例えば行列式を掛けて指紋コードを暗号化する場合に比べて解読し難くすることが可能である。

【0015】ここに、個人コードを用いた暗号化としては、例えば、指紋コードを64ビットの暗号文データとして生成し、個人コードを8ビットの数字4桁(64ビット)の暗号鍵(鍵ブロック)とし、DES(Data Encryption Standard)暗号方式を用いて指紋コードを暗号化することが好ましい。また、個人コードは、例えば、指紋登録システムの外部から入力されるように構成しても良く、また、RAMやROM等の記憶装置に予め記憶された個人コードを暗号化手段が読み出すように構成しても良い。

【0016】請求項3の発明は、請求項1の指紋登録システムが、前記コード化手段によって指紋コードが生成される指と異なる同一人の他の指の指紋コードを記録した暗号鍵記録手段をさらに備え、前記暗号化手段が、前記コード化手段によって指紋コードが生成された際に、前記暗号鍵記録手段に記録された前記他の指の指紋コードを暗号鍵として生成された指紋コードを暗号化することで特定したものである。

【0017】請求項2の発明において、個人コードを指紋登録システムの外部から入力する構成を探る場合には、この個人コード入力の際に個人コードが漏洩してしまうおそれがある。そこで、請求項3の発明は、指紋登録システム内に暗号鍵記録手段を設けることで、暗号鍵が他人に知られてしまうことを防止することとしたものである。ここに、暗号鍵記録手段は、請求項1の記録手段と同様に、例えばRAM等で構成できる。

【0018】請求項4の発明は、請求項2又は3記載の暗号化手段によって暗号化された指紋コードである暗号化コードを再暗号化する再暗号化手段をさらに備えたことで特定したものである。

【0019】請求項4の発明によれば、暗号化コードを再暗号化することにより、指紋の所有者である本人以外の第3者から指紋情報が漏洩した場合に、漏洩した指紋情報から指紋コードが解読できないようにすることができる。

【0020】請求項5の発明は、請求項4記載の再暗号化手段が、所定の第3者コードを暗号鍵として前記暗号化コードを再暗号化することで特定したものである。こ

こに、暗号化コードの再暗号化には、例えば、上述したDES暗号方式を用いることができる。

【0021】請求項6の発明は、請求項5記載の指紋登録システムが、前記第3者コードを記録した第3者コード記憶手段をさらに備えたことで特定したものである。

【0022】

【発明の実施の形態】以下、本発明の実施の形態を図に基づいて説明する。

【指紋登録システムの全体構成】図1は、本発明の実施形態による指紋登録システムの外観構成図である。図1において、指紋登録システムは、圧力式指紋センサ(以下、「指紋センサ」という)12及びIC(Integrated Circuit)13が組み込まれたICカード11と、ICカード11と電気的に接続され、処理装置15、ICカード11を差し込むICカード入力アダプタ16、記録部17、入力装置(例えば、キーボード、マウス等)18、及びディスプレイ(例えば、CRT、LCD等)29からなるコンピュータ14とから構成されている。

【0023】[ICカードの構成]図2は、図1に示したICカード11のハードウェアブロック図である。図2において、ICカード11は、上述した指紋センサ12と、上述したIC13を構成するMPU(Micro Processing Unit)21及びRAM(Random Access Memory)23と、外部コネクタ24とからなり、これらがバス25を介して相互に接続されている。

【0024】ここに、指紋センサ12には、特開平8-68704号(特許第2557795号)に記載されたアクティブマトリックス型面圧入力パネル(以下、「面圧入力パネル」という)100が用いられている。図3は、面圧入力パネル100の構成図である。図3において、面圧入力パネル100は、以下のように構成されている。即ち、面圧入力パネル100は、下面に導電膜102aを有する可撓性の圧力シート102を有している。また、面圧入力パネル100は、絶縁基盤110上にマトリックス状に走査電極130,140を配置し、この走査電極線130,140の交点ごとに薄膜トランジスタ120と導電接触板150とを形成することで構成した回路板103を有している。圧力シート102の導電膜102aは、回路板103の導電接触板150と対接するように位置づけて積層されている。また、薄膜トランジスタ120のゲートとドレインとがマトリックス状走査電極線130,140の一方と他方とにそれぞれ接続され、ソースが導電接触板150に接続されている。この面圧入力パネル100は、圧力シート102を押圧した指の指紋パターンを図示せぬ検出回路によって検出する。なお、指紋センサ12は、指紋パターンを得ることができるもの限り、どのような種類のものが用いられていても良い。

【0025】RAM23には、MPU21によって実行される各種のプログラム、MPU21によるプログラム

実行に際して使用される各種のデータ等が格納されている。また、RAM23は、MPU21の作業領域として使用される。

【0026】MPU21は、RAM23に格納されたプログラムを実行することによって、指紋センサ12により得られた指紋パターンについて、コード化処理、暗号化処理、識別番号付与処理、指紋データの記録処理、照合処理等を行う。外部コネクタ24は、インターフェイス回路等からなり、コンピュータ14との接続に際して使用される。

【0027】〔コンピュータの構成〕図4は、図1に示したコンピュータ14のハードウェアブロック図である。図2において、コンピュータ14は、記録部17と、入力装置18と、ディスプレイ29と、処理装置15に相当するCPU26、RAM28、ROM30と、ICカード入力アダプタ16に相当するICカードコネクタ27とが、バス31を介して相互に接続されることによって、構成されている。

【0028】ICカードコネクタ27は、ICカード11の外部コネクタ24(図2参照)と接続され、ICカード11とコンピュータ14との間におけるデータの入出力制御を行う。入力装置18は、コンピュータ14のオペレータがデータを入力するために使用される。ROM30は、CPU26によって実行されるプログラムや各種のデータを保持する。RAM28は、CPU26の作業領域をなし、CPU26の処理結果が記録される。CPU26は、ICカード11からのデータに対する処理を実行する。記録部17は、例えばフロッピーディスク(FD)ドライブを用いて構成されており、FDに対して書き込み／読み出し動作を行う。CPU26は、プログラムを実行することによって、ICカード11からのデータに係る処理等を行う。ディスプレイ29は、CPU26の処理結果に基づく画像、文字等を表示する。

【0029】〔指紋登録システムの機能〕図5は、図1～図4に示した指紋登録システムの機能ブロック図である。図1及び図2に示したICカード11は、指紋圧力入力部301、コード化部302、暗号化部303、指紋コード記録部304、入出力I/F部305、及び暗号鍵記録部(個人コード記録部)306からなる。

【0030】指紋圧力入力部301は、図2に示した指紋センサ12に相当し、自身に押し当てられた指の指紋パターンを読み取り、コード化部302へ与える。コード化部302は、指紋圧力入力部301から指紋パターンを受け取り、この指紋パターンから特徴点を抽出し、その相対座標値をコード化する。図6は、コード化部302による処理の説明図である。

【0031】コード化部302は、指紋圧力入力部301から指紋パターンの原画データ(図6(a)参照)を受け取る。すると、コード化部302は、原画データについて平準化処理を施す(図6(b)参照)。続いて、コード化

部302は、平準化処理が施された原画データを2値化画像データに変換する(図6(c)参照)。そして、コード化部302は、2値化画像データに対し細線化処理を施す(図6(d)参照)。この細線化処理によって得られたデータを指紋データと称する。続いて、コード化部302は、指紋データからマニューシャポイントと呼ばれる特徴点を複数個抽出し、抽出した特徴点の相対座標値をコード化する(例えば、64ビットのコードが生成される)。このコード化処理によって生成されたデータを指紋コードと称する。そして、コード化部302は、指紋コードを暗号化部303に与える。なお、指紋による本人照合処理の際には、この指紋コード、即ちマニューシャポイントの相対座標値が照合され、本人か否かの判定がなされる。

【0032】暗号化部303は、コード化部302から指紋コードを受け取り、この指紋コードに所定の行列式を掛けることによって、指紋コードを暗号化する。また、暗号化部303は、設定に応じて、入力装置18から入力される個人コード、或いは暗号鍵記録部306に記録された暗号鍵を用いて指紋コードを暗号化する。この暗号化部303による処理によって得られたデータを暗号化コードと称する。そして、暗号化部303は、暗号化コードを指紋コード記録部304に記録する。

【0033】指紋コード記録部304は、図2に示したRAM23に相当し、暗号化部303によって記録された暗号化コードを、照合元指紋データとして保持する。また、入出力I/F部305は、図2に示した外部コネクタ24に相当し、指紋コードデータ記録部304に保持されたデータを外部のコンピュータ14へ出力する際、或いは、コンピュータ14からデータを受け取る際のインターフェース部として機能する。

【0034】暗号鍵記録部306は、図2に示したRAM23に相当する。暗号鍵記録部306は、指紋コード記録部304に暗号化されて記録される指紋コードの指紋所有者の他の指に係る指紋コードを、暗号鍵として使用する個人コードとして保持している。この暗号鍵記録部306に保持された暗号鍵は、暗号化部303の処理に際して用いられる。なお、この暗号鍵記録部306には、上述した他の指の指紋コードに代えて、指紋所有者の所定の個人コード(例えば、数字4桁の64ビットのコード)が保持されるように構成されていても良い。

【0035】また、図5において、図1及び図4に示したコンピュータ14は、入出力I/F部311、指紋コード記録部データ読取部(以下、「データ読取部」という)312、再暗号化部313、第3者指紋コード記録部314、コード入力部315、及び第3者コード記録部316からなる。

【0036】入出力I/F部311は、図4に示したICカードコネクタ27に相当し、コンピュータ14内のデータをICカード11に与える。一方、ICカード1

1からのデータを受け取る。

【0037】データ読取部312は、ICカード11内の指紋コード記録部304に記録された暗号化コードを読み出して、再暗号化部313に与える。再暗号化部313は、データ読取部312から暗号化コードを受け取った場合に、第3者コード記録部316に保持された第3者コードを暗号鍵として暗号化コードを再暗号化することによって、再暗号化コードを生成する。この再暗号化コードを第3者指紋コードと称する。なお、再暗号化部313は、コード化部302によって生成された指紋コードをICカード11から取得して暗号化するように構成されていても良い。

【0038】第3者指紋コード記録部314は、再暗号化部313による処理結果(第3者指紋コード)を保持する。また、第3者コード記録部316は、再暗号化部313の処理に使用される暗号鍵として、第3者(例えばクレジットカード会社等)のコード(例えば数字4桁の64ビットのコード)たる第3者コードを予め保持している。

【0039】コード入力部315は、図1及び図4に示した入力装置18に相当し、暗号化部303による処理に使用される個人コードの入力に使用される。また、指紋コード記録部317には、指紋コード記録部データ読取部312によって、ICカード304から読み出された暗号化コードが記録される。

【0040】なお、図5において、第3者指紋コード記録部314、第3者コード記録部316、及び指紋コード記録部317は、図4に示したRAM28或いは記録部17に装着されるFDに相当する。また、図5において、コード化部302、暗号化部303、データ読取部312、及び再暗号化部313は、図2に示したMPU21或いは図4に示したCPU26がプログラムを実行することによって実現する機能である。

【0041】〔指紋登録システムによる処理〕図7は、図5に示した指紋登録システムによる処理を示すフローチャートである。図7に示す処理は、図1に示したICカード11がICカード入力アダプタ16に差し込まれ、コンピュータ14の電源が投入され、指紋コードを登録すべき者がICカード11の指紋センサ12(指紋圧力入力部301)を所定の指で押圧することによってスタートする。

【0042】図7において、処理がスタートすると、最初に、指紋センサ12によって指紋パターンが読み取られ、指紋パターンの原画データが取得される(S01)。すると、コード化部302が、原画データに対し、平準化処理を施し(S02)、2値化処理及び細線化処理を施す(S03)。これによって、指紋データが得られる。続いて、コード化部302が、指紋データから複数個の特徴点(マニューチャポイント)を抽出し、この特徴点の相対座標値をコード化する(S05)。このS05の処理に

よって生成された指紋コード(64ビット)は、暗号化部303に与えられる。

【0043】S05の処理が終了すると、図1に示したディスプレイ29には、暗号化部303による処理に使用される個人コードをコード入力部315(入力装置18)から入力するか否かの指示を求める画面(図示せず)が、表示される。このとき、コンピュータ14のオペレータが、個人コードを入力する旨の指示を入力装置18から入力した場合(S06; YES)には、処理がS07へ進む。これに対し、オペレータが個人コードを入力しない旨の指示を入力した場合には、処理がS08へ進む。

【0044】処理がS07へ進んだ場合には、ディスプレイ29には、オペレータに対して個人コードの入力を促す画面(図示せず)が表示される。これに対し、オペレータが個人コード(数字4桁の64ビットのコード)をコード入力部315から入力すると、その個人コードは、入出力I/F部311、入出力I/F部305を介して暗号化部303に与えられる。すると、暗号化部303は、個人コードを暗号鍵とし、コード化部302から受け取った指紋コードをDES暗号方式に従って暗号化する。これによって、暗号化コードが生成される。そして、暗号化部303は、生成した暗号化コードを指紋コード記録部304へ書き込む(S11)。これによって、暗号化コードがICカード11に登録される。

【0045】一方、処理がS08へ進んだ場合には、ディスプレイ29には、オペレータに対して、個人コードを自動入力するか否かの指示を求める画面(図示せず)が、表示される。このとき、オペレータが、例えば個人コードを自動入力する旨の指示を入力装置18から入力した場合(S08; YES)には、処理がS09へ進む。これに対し、オペレータが個人コードを自動入力しない旨の指示を入力した場合(S08; NO)には、処理がS10へ進む。

【0046】処理がS09へ進んだ場合には、暗号化部303には、個人コードを自動入力する旨の指示が与えられる。すると、暗号化部303は、暗号鍵記録部306に保持されている他の指の指紋コード(64ビット)を読み出し、この他の指の指紋コードを暗号鍵とし、コード化部302から受け取った指紋コードをDES暗号方式に従って暗号化する。これによって、暗号化コードが生成される。そして、暗号化部303は、生成した暗号化コードを指紋コード記録部304に書き込む(S11)。これによって、暗号化コードがICカード11に登録される。

【0047】一方、処理がS10へ進んだ場合には、暗号化部303には、個人コードを自動入力しない旨の指示が与えられる。すると、暗号化部303は、コード化部302から受け取った指紋コードに所定の行列式を掛けることによって、暗号化コードを生成する。そして、

暗号化部303は、暗号化コードを指紋コード記録部304に書き込む(S11)。これによって、暗号化コードがICカード11に登録される。

【0048】このように、S01～S11の処理によって、指紋データを暗号化した暗号化コードがICカード11に登録される。その後、ディスプレイ29には、暗号化コードを再暗号化するか否かの指示を求める画面(図示せず)が、表示される。これに対し、オペレータが再暗号化を行う旨の指示を入力装置18から入力した場合(S12; YES)には、処理がS13へ進む。これに対し、オペレータが再暗号化しない旨の指示を入力した場合(S12: NO)には、データ読取部312が、指紋コード304から暗号化コードを読み出し、コンピュータ14内の指紋コード記録部317に書き込み(S15)、指紋登録システムによる処理を終了する。このS15の処理によって、暗号化コードがコンピュータ14に登録される。

【0049】処理がS13へ進んだ場合には、再暗号化を行う旨の指示がデータ読取部312に与えられる。すると、データ読取部312が、指紋コード記録部304に保持されている暗号化コードを読み出し、再暗号化部313に与える。

【0050】すると、再暗号化部313が、第3者コード記録部316に保持されている所定の第3者コード(64ビット)を読み出し、この第3者コードを暗号鍵とし、データ読取部312から受け取った暗号化コードをDES暗号方式に従って暗号化する。これによって、再暗号化コードたる第3者指紋コードが生成される(S14)。

【0051】そして、再暗号化部313が、S14にて生成した第3者指紋コードを第3者指紋コード記録部314に書き込む(S15)。これによって、暗号化コードをさらに暗号化した第3者指紋コードがコンピュータ14に登録される。このS15の処理が終了すると、指紋登録システムによる処理が終了する。このように、S12～S15の処理によって、暗号化コード或いは第3者指紋コードがコンピュータ14に登録される。

【0052】その後、指紋圧力入力部301が指で押されると、図6に示したS01～S05の処理が実行され、照合対象となる指紋コードが得られる。ここで、指紋登録システムにICカード11内で指紋照合(本人照合)を行う設定がなされている場合には、ICカード11のMPU21(図2参照)が、指紋コード304に保持された暗号化コードを読み出し、この暗号化コードを復号して照合元の指紋コードを得る。そして、照合元の指紋コードと照合対象の指紋コードとを対比する。

【0053】これに対し、指紋登録システムにコンピュータ14内で指紋照合を行う設定がなされている場合には、コンピュータ14のCPU26が、指紋コード317から該当する暗号化コードを読み出して照合元の指紋

コードに復号化し、ICカード11から受け取った照合対象の指紋コードと対比する。

【0054】或いは、指紋登録システムに第3者指紋コードで指紋照合を行う設定がなされている場合には、コンピュータ14のCPU26が、第3者指紋コード記録部314から該当する第3者指紋コードを読み出して照合元の指紋コードに復号化し、ICカード11から受け取った照合対象の指紋コードと対比する。

【0055】そして、両者が合致する場合には、CPU26は、例えばディスプレイ29に、指紋が合致した旨、或いは本人であることが確認できた旨を示す画面(図示せず)を表示させる。一方、両者が合致しない場合には、CPU26は、ディスプレイ29に、指紋が合致しない旨、或いは本人でない旨を示す画面(図示せず)を表示させる。

【0056】〔実施形態の効果〕本実施形態による指紋登録システムによると、指紋センサ12(指紋圧力入力部301)で読み取られた指紋パターンが、コード化部302にてコード化され(S05)、所定の行列式を掛けることによって暗号化され(S10)、指紋コード記録部317に登録される(S11)。

【0057】このように、本実施形態によれば、指紋コードを暗号化するので、他人がICカード11から暗号化コードを得ても指紋コードを知ることはできない。従って、個人の指紋情報を他人へ知られることなく指紋照合を行うことができ、指紋照合システムの普及促進を図ることができる。

【0058】また、本実施形態による指紋登録システムによると、オペレータの選択によって、暗号化部303は、入力装置18から入力された個人コードを暗号鍵として用い、指紋コードに対する暗号化処理を行う(S06, S07)。このため、暗号化部303が指紋コードに行列式を掛けて暗号化する場合に比べ、解読困難な暗号化コードをICカード11に登録することができる。

【0059】また、本実施形態による指紋登録システムによると、オペレータの選択によって個人コードを自動入力する設定ができる(S08)。この場合には、暗号化部303が、暗号鍵記録部306から他の指の指紋コードを読み出し、この他の指の指紋コードを暗号鍵として用い、指紋コードに対する暗号化処理を行う(S09)。このため、複雑な個人コードをコード入力部315から入力する煩雑さを回避することができ、逐一個人コードを入力することを回避して、個人コードの機密保護向上を図ることができる。これによって、個人の指紋情報をICカード11で容易に暗号化でき、かつ信頼性の高いセキュリティを実現できる。

【0060】さらに、本実施形態による指紋登録システムによると、オペレータの選択によって、再暗号化部313が暗号化コードを再暗号化した第3者指紋コードを生成し、第3者指紋コード記録部314に記録する(S

S12～S15)。従って、コンピュータ14が、例えばクレジットカード会社や電子マネーの取引先等に設置され、クレジットカード会社等において顧客の指紋照合を行う場合には、上述したS12～S15の処理が実行されるようすれば、個人(顧客)の指紋情報の機密性をさらに高めることができる。

【0061】このように、本実施形態による指紋登録システムによると、多人数の個人についての指紋照合システムを構築する場合に、各個人の指紋情報の機密を保持することができる。

【0062】なお、本実施形態による指紋登録システムでは、暗号化部303、及び暗号鍵記録部306をICカード11内に設けたが、これらは、コンピュータ14内に設けられていても良い。

【0063】

【発明の効果】以上説明したように、本発明による指紋登録システムによれば、従来に比べて個人の指紋情報の漏洩を防ぐことができ、さらに多数の指紋情報を取り扱う第3者での指紋情報の機密保持を実現できる。

【図面の簡単な説明】

【図1】本発明の実施形態による指紋登録システムの外観構成図

【図2】図1に示したICカードのハードウェア構成図

【図3】図2に示した指紋センサの構成図

【図4】図1に示したコンピュータのハードウェア構成図

【図5】図1に示した指紋登録システムの機能ブロック図

【図6】図5に示したコード化部の処理説明図

【図7】図1に示した指紋登録システムによる処理を示すフローチャート

【符号の説明】

11 ICカード

12 圧力式指紋センサ

13 IC(コード化手段、暗号化手段、記録手段)

14 コンピュータ

16 ICカードコネクタ

21 MPU

23 RAM

26 CPU(再暗号化手段)

28 RAM

302 コード化部(コード化手段)

303 暗号化部(暗号化手段)

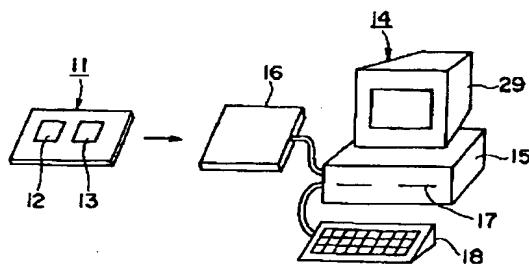
304 指紋コード記録部(記録手段)

306 暗号鍵記録部(暗号鍵記録手段)

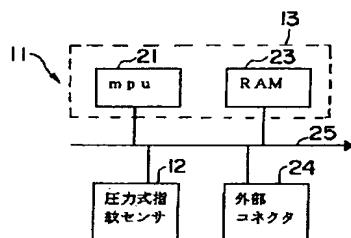
313 再暗号化部(再暗号化手段)

314 第3者コード記録部(第3者コード記憶手段)

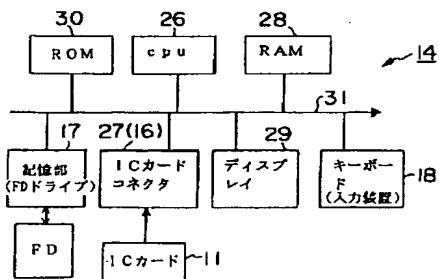
【図1】



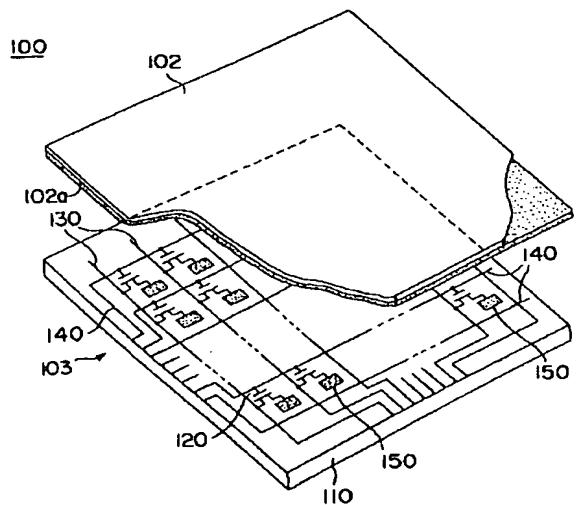
【図2】



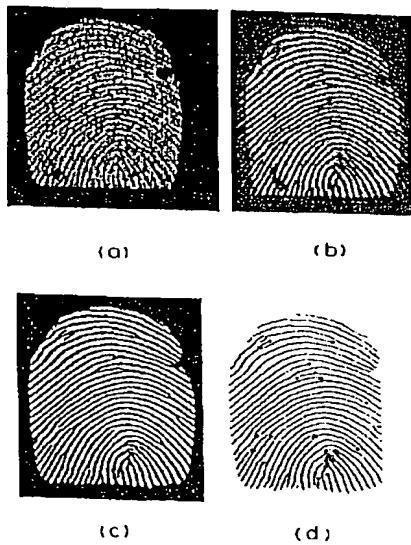
【図4】



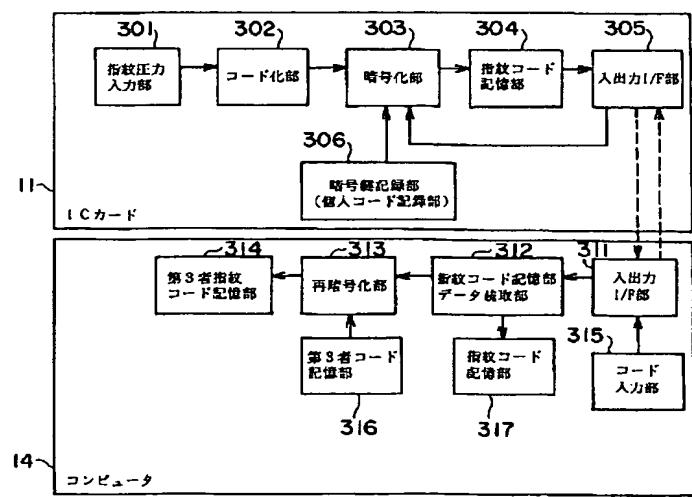
【図3】



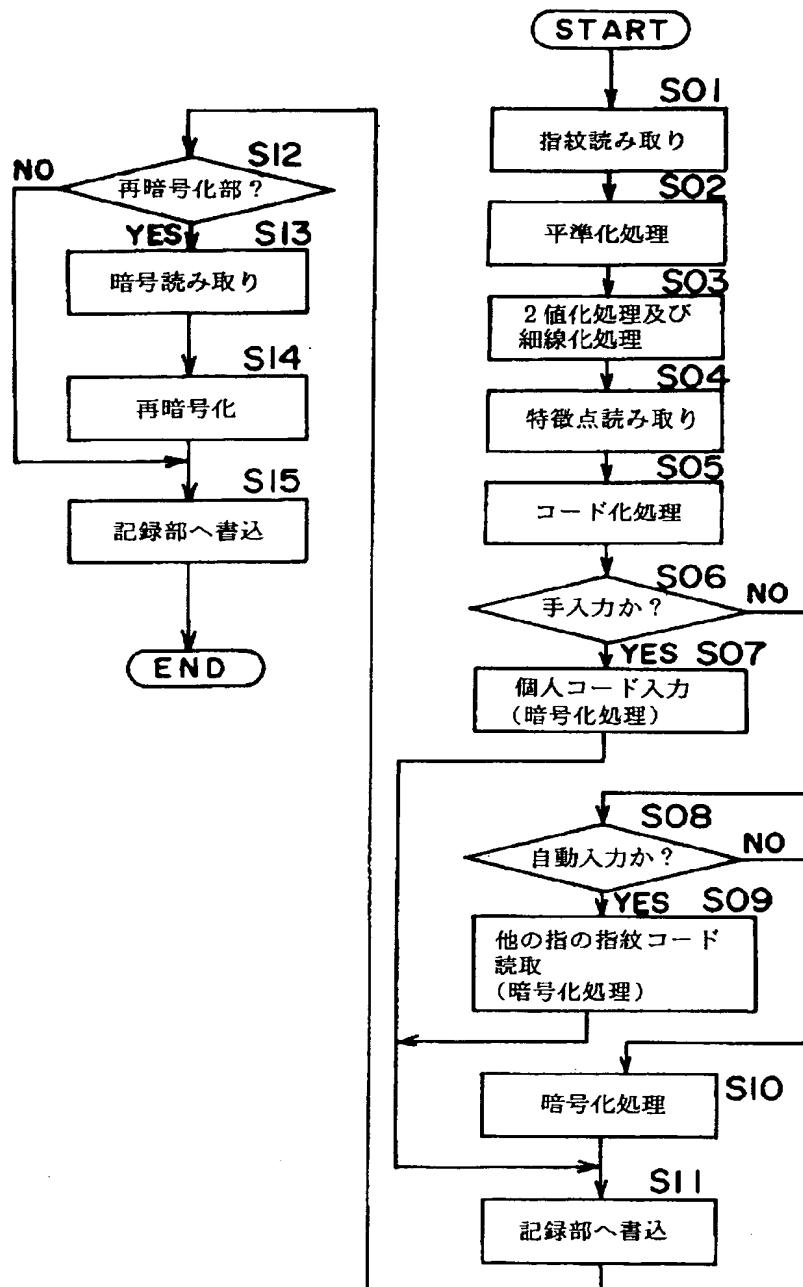
【図6】



【図5】



【図7】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.